International Journal of Algebra, Vol. 7, 2013, no. 2, 79 - 90
HIKARI Ltd, www.m-hikari.com

Minimal Cyclic Codes of Length $2p^n$

Seema Rani and Pankaj Kumar

Dept. of Mathematics, G.J. U.S&T
Hisar-12500, India
bharseema@gmail.com

Inderjit Singh

Dept. of Mathematics, D.N.Collge
Hisar-125001, India

Abstract

Explicit expressions for all 2(nd+1) primitive idempotents in the ring $R_{2p^n} = GF(l)[x]/<x^{2p^n}-1>$, where p and l are distinct odd primes such that $o(l)_{2p^n} = \phi(2p^n)/d$, $d \geq 1$ an integer, are obtained. The minimum distance, generating polynomials and dimension of the minimal cyclic codes generated by these primitive idempotents are also discussed. As example, we discuss the parameters of the minimal cyclic codes of length 22.

Mathematics Subject Classification: 11A03; 15A07; 11R09; 11T06; 11T22; 11T71; 94B05; 94B15

Keywords: Cyclotomic cosets; Primitive idempotents; Minimal cyclic codes; Generating polynomials;Minimum distance and Dimension

1. Introduction

Let F be a field of odd prime order l and k ≥1 be an integer such that gcd(l, k)=1. Let $R_k = \frac{GF(l)[x]}{<x^k-1>}$. Then, R_k is semi-simple. As, every ideal in R_k is the direct sum of its minimal ideals. Hence, to describe the complete set of ideals (codes over F) in R_k, it is sufficient to find its complete set of primitive idempotents. Let $o(l)_k$ denotes the order of l modulo k. For k = 2, 4, p^n, $2p^n$, p is odd prime and $o(l)_k = \phi(k)$, the complete set of primitive idempotents in R_k are obtained by Arora and Pruthi [4,9]. $k=p^n$, $2p^n$ ($n \geq 1$), p odd prime and $o(l)_k = \frac{\phi(k)}{2}$, the complete set of primitive idempotents in R_k are obtained by Batra, Arora [8]. For $k = p^n q$ ($n \geq 1$), p and q distinct odd primes where l is primitive root modulo p^n and q both with $\gcd(\phi(2p^n), \phi(q)) = 2$, the primitive idempotents in R_k are obtained by Bakshi and Raka [3]. For $k = p^n$ ($n \geq 1$), p odd prime, $o(l)_k = \frac{\phi(k)}{e}$, e is positive integer, the primitive idempotents in R_k are obtained by Sharma, Raka and Dumir [5]. Ranjeet Singh and Manju Pruthi [6] obtain the primitive idempotents of the quadratic residue codes of length $p^n q^m$, p, q are distinct odd primes and $o(l)_{p^n} = \frac{\phi(p^n)}{2}, o(l)_{q^m} = \frac{\phi(q^m)}{2}$, $\gcd(\frac{\phi(p^n)}{2}, \frac{\phi(q^m)}{2}) = 1$. Amita Sahni and P.T. Sehgal [1] describe the primitive idempotents of minimal cyclic codes of length $p^n q$, p, q are distinct odd primes and, $o(l)_{p^n} = \phi(p^n), o(l)_q = \phi(q)$, $\gcd(\phi(p^n), \phi(q)) = d$, p does not divide q-1.

In this paper, we have extended the results of Batra, Arora [8]. We consider the case when $k = 2p^n$, where p and l are distinct odd primes, $o(l)_{2p^n} = \phi(2p^n)/d$, $d \geq 1$ an integer. We obtain explicit expressions for all the 2(nd+1) primitive idempotents in R_k. The minimum distance, generating polynomials and dimension of the minimal cyclic codes generated by these primitive idempotents are also discussed. In Section2 (Lemmas 1- 9 and Theorem 1), we discuss the cyclotomic cosets modulo $2p^n$ and some basic results for describing the primitive idempotents in R_k. In Section 3(Theorem 3), the explicit expression of primitive idempotents have obtained. In Section 4 (Theorem 4-6), we discuss the dimension, generating polynomial and minimum distance of minimal cyclic codes of length $2p^n$**.** In section 5, we discuss the various parameters of minimal cyclic codes of length 22.

2. Primitive idempotents in $R_{2p^n} = \frac{GF(l)[x]}{< x^{2p^n} - 1 >}$ and minimal cyclic codes of length $2p^n$ over F(=GF(l))

In this section we describe the minimal cyclic codes of length $2p^n$ over F, where p and l are distinct odd primes and $o(l)_{2p^n} = \phi(2p^n)/d$, $d \geq 1$ an integer. A set of $\phi(n)$ integers $a_1, a_2, \ldots, a_{\phi(n)}$, where $\gcd(a_i, n) = 1$ and $a_i \not\equiv a_j \pmod{n}$ for all i, j, $1 \leq i, j \leq \phi(n)$, $i \neq j$ form a reduced residue system modulo n. Let l be a positive integer of order $\phi(n)$, then l is called primitive root modulo n. We know that primitive root modulo n exists only when n = 2, 4, p^e, $2p^e$ where p is an odd prime.

Lemma 1. Let p and l be distinct odd primes and $n \geq 1$ be an integer .

If $o(l)_{2p^n} = \phi(2p^n)/d$, then $o(l)_{2p^{n-j}} = \dfrac{\phi(2p^{n-j})}{d}$, for all $0 \leq j \leq n-1$.

Proof. Trivial.

Lemma 2. There exists a positive integer g, 1 < g < 2p, such that gcd (g, 2pl) = 1, and $o(g)_{2p} = \phi(p)$, where g, g^2, …, $g^{d-1} \notin \{1, l, l^2, \ldots, \ell^{\frac{\phi(2p)}{d}-1}\}$.

Proof. See [1, Lemma4].

Lemma 3. There exists a positive integer g, 1 < g < 2p, such that gcd (g, 2pl) = 1and $g^i \not\equiv l^k$ (mod 2p) for any i, k; $1 \leq i \leq d-1$ and $0 \leq k \leq \dfrac{\phi(p)}{d}$. Further, for any j, $1 \leq j < n$, the set $\{1, l, l^2, \ldots, \ell^{\frac{\phi(p^{n-j})}{d}-1}$, g, g$l$, g$l^2$ …, $g\ell^{\frac{\phi(p^{n-j})}{d}-1}$,..., g^{d-1}, $g^{d-1}l$, $g^{d-1}l^2$,…, $g^{d-1}\ell^{\frac{\phi(p^{n-j})}{d}-1}\}$ form a reduced residue system modulo $2p^{n-j}$.

Proof. Trivial.

Let S = {0, 1, 2,…, $2p^n$ -1}. For a, b $\in$ S, say that a ~b iff $a \cong b\, l^i$ (mod $2p^n$) for some integer $i \geq 0$.This defines an equivalence relation on the set S. The equivalence classes due to this relation are called l-cyclostomic cosets modulo $2p^n$. The l -cyclotomic coset containing $s \in S$ is denoted by

$C_s = \{s, sl, sl^2, \ldots, sl^{t_s-1}\}$,

where t_s is the least positive integer such that $sl^{t_s} \equiv s$(mod $2p^n$) and $|C_s|$ denotes the order of the l-cyclotomic coset C_s, containing s.

Theorem 1. If p is an odd prime $o(l)_{2p^n} = \phi(2p^n)/d$, $d \geq 1$ an integer, then for the integer $n \geq 1$, there are 2(nd+1) cyclotomic cosets (mod $2p^n$) given by

(i) $C_0 = \{0\}$

(ii) $C_{p^n} = \{p^n\}$

For $0 \leq j \leq n-1$, $0 \leq k \leq d-1$

(iii) $C_{g^k p^j} = \{g^k p^j, g^k p^j l, \ldots, g^k p^j \ell^{\frac{\phi(p^{n-j})}{d}-1}\}$

(iv) $C_{2g^k p^j} = \{2g^k p^j, 2g^k p^j l, \ldots, 2g^k p^j \ell^{\frac{\phi(p^{n-j})}{d}-1}\}$,

where g is the fixed integer as defined in Lemma 2.

Proof. Trivial.

Note 1. (i) $g^u \in C_1$, for any integer u if and only if u ≡ 0 (mod d).

(ii) $-1 \in C_1$ or $-1 \in C_{g^{d/2}}$, if $-1 \in C_1$ then $-C_1 = C_1$ otherwise $-C_1 = C_{g^{d/2}}$.

(iii) If $-C_1 = C_1$ then $-C_{g^k p^i} = C_{g^k p^i}$, otherwise $-C_{g^k p^i} = C_{g^{k+d/2} p^i}$ for all i, k; $0 \le i \le n-1$ and $0 \le k \le d-1$.

Lemma 4. For any odd prime p and positive integer k, if β is primitive p^k th root of unity in some extension field of GF(l) and $o(l)_{p^k} = \phi(p^k)$ (mod p^k), then

$$\sum_{s=0}^{\phi(p^k)-1} \beta^{l^s} = \begin{cases} -1 & \text{if } k = 1 \\ 0 & \text{if } k > 1. \end{cases}$$

Proof. See [3, Lemma 4].

Lemma 5. For any odd prime p and positive integer k, if β is primitive $2p^k$ th root of unity in some extension field of GF(l) and $o(l)_{2p^k} = \phi(2p^k)$ (mod $2p^k$), then

$$\sum_{s=0}^{\phi(2p^k)-1} \beta^{l^s} = \begin{cases} 1 & \text{if } k = 1 \\ 0 & \text{if } k > 1. \end{cases}$$

Proof. Similar as Lemma 4.

Let α is primitive $2p^n$th root of unity in some extension field of GF(l). For $0 \le i \le n-1$ and $0 \le k \le d-1$, define $A_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{2p^i s}$ and $B_i^{(k)} = \sum_{s \in C_{g^k}} \alpha^{p^i s}$ .Since $C_{g^k l} = C_{g^k}$, therefore $(A_i^{(k)})^l = A_i^{(k)}$, so that each $A_i^{(k)}, B_i^{(k)} \in GF(l)$.

Lemma 6. For each i, $0 \le i \le n-1$, $\sum_{k=0}^{d-1} A_i^{(k)} = \begin{cases} 0 & \text{if } i \le n-2 \\ -p^{n-1} & \text{if } i = n-1. \end{cases}$

Proof. See [1, Lemma 10].

Lemma 7. For each i, $0 \le i \le n-1$, $\sum_{k=0}^{d-1} B_i^{(k)} = \begin{cases} 0 & \text{if } i \le n-2 \\ p^{n-1} & \text{if } i = n-1. \end{cases}$

Proof. Similar as above.

Lemma 8. For each h, k, $0 \le h, k \le d-1$, $0 \le i, j \le n$,

$$\sum_{s \in C_{g^h p^j}} \alpha^{2g^k p^i s} = \begin{cases} 1 & \text{if } i+j \ge n,\ j = n, \\ \dfrac{\phi(p^{n-j})}{d} & \text{if } i+j \ge n,\ j \le n-1, \\ \dfrac{1}{p^j} A_{i+j}^{(h+k)} & \text{if } i+j \le n-1. \end{cases}$$

Proof. Case (i) For j = n, i + j ≥ n, $C_{g^h p^j} = C_{g^k p^n} = C_{p^n}$, So, $\sum_{s\in C_{p^n}} \alpha^{2g^k p^i s} = 1$.

Case (ii) Let i + j ≥ n and j ≤ n – 1, then the above sum equals $\dfrac{\phi(p^{n-j})}{d}$.

Case (iii) If i + j ≤ n –1, then $\sum_{s\in C_{g^h p^j}} \alpha^{2g^k p^i s} = \sum_{s=0}^{\frac{\phi(2p^{n-j})}{d}-1} \beta^{l^s}$, where $\beta = \alpha^{2g^{(h+k)} p^{i+j}}$, then β is primitive p^{n-i-j} th root of unity. Therefore, $\beta^{l^r} = \beta^{l^s}$, if and only if $l^r \equiv l^s$ (mod p^{n-i-j}), if and only if r ≡ s (mod $\dfrac{\phi(p^{n-i-j})}{d}$).

Then $\sum_{s=0}^{\frac{\phi(2p^{n-j})}{d}-1} \beta^{l^s} = p^i \sum_{s=0}^{\frac{\phi(p^{n-i-j})}{d}-1} \beta^{l^s}$. Also,

$$A_{i+j}^{(h+k)} = \sum_{s\in C_{g^{h+k}}} \alpha^{2p^{i+j}s} = \sum_{s=0}^{\frac{\phi(2p^n)}{d}-1} \beta^{l^s} = \frac{\phi(2p^n)}{d}.\frac{d}{\phi(p^{n-i-j})} \sum_{s=0}^{\frac{\phi(p^{n-i-j})}{d}-1} \beta^{l^s} = \frac{1}{p^{i+j}} A_{i+j}^{(h+k)}$$

Then, by above discussion we get the required sum.

Lemma 9. For each h, k, 0≤ h, k ≤ d–1, 0 ≤ i, j ≤ n,

$$\sum_{s\in C_{g^h p^j}} \alpha^{g^k p^i s} = \begin{cases} -1 & \text{if } i+j \ge n,\ j=n, \\ -\dfrac{\phi(p^{n-j})}{d} & \text{if } i+j \ge n,\ j \le n-1, \\ \dfrac{1}{p^j} B_{i+j}^{(h+k)} & \text{if } i+j \le n-1. \end{cases}$$

Proof. Similar as Lemma 8.

3. Evaluation of primitive idempotents

If α is a primitive mth root of unity in some extension field GF(l), then the polynomial $M^{(s)}(x) = \Pi_{i\in C_s}(x-\alpha^i)$ is the minimal polynomial over GF(l). Let Ω_s be the minimal ideal in R_m generated by $\frac{x^m-1}{M^s(x)}$ and $\theta_s(x)$ be the primitive idempotent of Ω_s and define $\sigma_s(x) = \sum_{i\in C_s} x^i$.

Theorem 2. $\theta_s(x) = \sum_{i=0}^{m-1} \varepsilon_i x^i$, where $\varepsilon_i = \sum_{j\in C_s} \alpha^{-ij}$ for all $i \geq 0$.

Proof. See [1, Theorem 1].

Theorem 3. The 2 (nd+1) primitive idempotents in R_{2p^n} are given by

(i) $\theta_0(x) = \frac{1}{2p^n}(1+x+x^2+...+x^{2p^n-1})$

(ii) $\theta_{p^n}(x) = \frac{1}{2p^n}\left\{1-\sigma_{p^n}(x)\right\} + \frac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}(\sigma_{2g^k p^i}(x) - \sigma_{g^k p^i}(x))\right\}$

(iii) For $0 \leq j \leq n-1$, $0 \leq k \leq d-1$,

$$\theta_{g^k p^j}(x) = \frac{p-1}{2p^{j+1}d}\left\{1-\sigma_{p^n}(x) + \sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}(\sigma_{2g^h p^i}(x) - \sigma_{g^h p^i}(x))\right\} +$$
$$\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}(B_{i+j}^{(\gamma+h)}\sigma_{g^h p^i}(x) + A_{i+j}^{(\gamma+h)}\sigma_{2g^h p^i}(x))$$

(iv) For $0 \leq j \leq n-1$, $0 \leq k \leq d-1$,

$$\theta_{2g^k p^j}(x) = \frac{p-1}{2p^{j+1}d}\left\{1+\sigma_{p^n}(x) + \sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x))\right\} +$$
$$\frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}A_{i+j}^{(\gamma+h)}(\sigma_{g^h p^i}(x) + \sigma_{2g^h p^i}(x)).$$

Proof. (i) By Theorem 2, $\theta_0(x) = \sum_{r=0}^{2p^n-1}\varepsilon_r x^r$, where $\varepsilon_r = \frac{1}{2p^n}\sum_{s\in C_0}\alpha^{-rs} = \frac{1}{2p^n}$ for all r.

Therefore, $\theta_0(x) = \frac{1}{2p^n}(1+x+x^2+...+x^{2p^n-1})$.

(ii) By Theorem 2, $\theta_{p^n}(x) = \sum_{r=0}^{2p^n-1}\varepsilon_r x^r$, where $\varepsilon_r = \frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{-rs}$. Since by Note 1, $-C_{p^n} = C_{p^n}$, therefore, $\varepsilon_r = \frac{1}{2p^n}\sum_{s\in C_{p^n}}\alpha^{rs}$. Now, $\varepsilon_0 = \frac{1}{2p^n}$, $\varepsilon_{p^n} = -\frac{1}{2p^n}$

For $0 \leq i \leq n-1$, $0 \leq k \leq d-1$, by using Lemma 8 and Lemma 9, we have

$$\varepsilon_{g^k p^i} = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{g^k p^i s} = -\frac{1}{2p^n},\ \varepsilon_{2g^k p^i} = \frac{1}{2p^n}\sum_{s\in C_{p^n}} \alpha^{2g^k p^i s} = \frac{1}{2p^n q}.$$

Thus, $\theta_{p^n}(x) = \frac{1}{2p^n}\left\{1-\sigma_{p^n}(x)\right\} + \frac{1}{2p^n}\left\{\sum_{k=0}^{d-1}\sum_{i=0}^{n-1}(\sigma_{2g^k p^i}(x)-\sigma_{g^k p^i}(x))\right\}.$

(iii) For $0 \le j \le n-1$, $0 \le k \le d-1$,

If $\theta_{g^k p^j}(x) = \sum_{r=0}^{2p^n-1}\varepsilon_r^{(k,j)} x^r$ **,** then by Theorem 2 and Note 1, $\varepsilon_r^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^k p^j}} \alpha^{-rs} =$ $= \frac{1}{2p^n}\sum_{s\in C_{g^{k+u} p^j}} \alpha^{rs}$, u = 0 or u = d/2 according as $-1\in C_1$ or $-1\in C_{g^{d/2}}$. Thus, $\varepsilon_r^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}} \alpha$, where $\gamma \equiv k+u \pmod d$ and $0 \le \gamma \le d-1$. Now,

$$\varepsilon_0^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}} \alpha^0 = \frac{\phi(2p^{n-j})}{2p^n d},\ \varepsilon_{p^n}^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}} \alpha^{p^n s} = -\frac{\phi(p^{n-j})}{2p^n d}.$$

For $0 \le i \le n-1$, by using Lemma 8 and Lemma 9, we have

$$\varepsilon_{g^h p^i}^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}} \alpha^{g^h p^i s} = \frac{1}{2p^n}\begin{cases} -\dfrac{\phi(p^{n-j})}{d} & \text{if } i \ge n-j,\ j \le n-1,\\[2mm] \dfrac{1}{p^j} B_{i+j}^{(h+k)} & \text{if } i \le n-j-1.\end{cases}$$

$$\varepsilon_{2g^h p^i}^{(k,j)} = \frac{1}{2p^n}\sum_{s\in C_{g^\gamma p^j}} \alpha^{2g^h p^i s} = \frac{1}{2p^n}\begin{cases} \dfrac{\phi(p^{n-j})}{d} & \text{if } i \ge n-j,\ j \le n-1,\\[2mm] \dfrac{1}{p^j} A_{i+j}^{(h+k)} & \text{if } i \le n-j-1.\end{cases}$$

Thus

$$\theta_{g^k p^j}(x) = \frac{p-1}{2p^{j+1}d}\left\{1-\sigma_{p^n}(x)+\sum_{h=0}^{d-1}\sum_{i=n-j}^{n-1}(\sigma_{2g^h p^i}(x)-\sigma_{g^h p^i}(x))\right\} + \frac{1}{2p^{n+j}}\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}(B_{i+j}^{(\gamma+h)}\sigma_{g^h p^i}(x)+A_{i+j}^{(\gamma+h)}\sigma_{2g^h p^i}(x)).$$

Similarly, we can evaluate $\theta_{2g^k p^j}(x)$.

Lemma 10. For $0 \le i \le n-1$, $0 \le k \le d-1$, then

(i) $A_i^{(k)} = 0$, if $0 \le i < n-1$.

(ii) $\sum A_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(\kappa-1)}{2}, & \text{if k is even; } p=\kappa^2\\[2mm] -p^{n-1}\dfrac{(1+\kappa)}{2}, & \text{if k is odd,}\end{cases}$ where d/2 is even.

(iii) $\sum A_{n-1}^{(k)} = \begin{cases} -p^{n-1}\dfrac{(1+\tau)}{2}, & \text{if } k \text{ is even; } -p=\tau^2 \\ p^{n-1}\dfrac{(\tau-1)}{2}, & \text{if } k \text{ is odd,} \end{cases}$ where d/2 is odd.

Proof. Using Lemma 8 and putting all values of $\sigma_{p^n}(\alpha^{2g^k p^j})$, $\sigma_{g^h p^i}(\alpha^{2g^k p^j})$ and $\sigma_{2g^h p^i}(\alpha^{2g^k p^j})$. in $\theta_{2g^k p^j}(\alpha^{2g^k p^j}) = 1$, we get

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j}^{(k+h)} = \frac{p^{n-1}((d-1)p+1)}{d}. \qquad (1)$$

On the similar lines

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j}^{(m+h)} = \frac{p^{n-1}(1-p)}{d}. \qquad (2)$$

$$\sum_{h=0}^{d-1}\sum_{i=0}^{n-j-1}\frac{1}{p^{i+j}}A_{i+j}^{(k+h+u)}A_{i+j-s}^{(k+h)} = 0. \qquad (3)$$

Also, we can solve above three equations for particular value j = n-1. Then these equations read as

$$\sum_{h=0}^{d-1}A_{n-1}^{(k+h+u)}A_{n-1}^{(k+h)} = \frac{p^{2n-2}((d-1)p+1)}{d}, \qquad (4)$$

$$\sum_{h=0}^{d-1}A_{n-1}^{(k+h+u)}A_{n-1}^{(m+h)} = \frac{p^{2n-2}(1-p)}{d}, \qquad (5)$$

$$\sum_{h=0}^{d-1}A_{n-1}^{(k+h+u)}A_{n-1-s}^{(m+h)} = 0, \text{ for all } 1 \le s \le n-1.$$

In view of above discussion, we conclude that,

$$\sum_{h=0}^{d-1}A_{j}^{(k+h+u)}A_{j}^{(k+h)} = 0,\ \sum_{h=0}^{d-1}A_{j}^{(k+h+u)}A_{j}^{(m+h)} = 0 \text{ and } \sum_{h=0}^{d-1}A_{j}^{(k+h+u)}A_{j-s}^{(m+h)} = 0,$$

for all $0 \le s \le j < n-1$, $0 \le k, m \le d-1$.

(i) By [1, Lemma 14], we have $A_j^{(k)} = 0$ for all $0 \le j < n-1$ and $0 \le k \le d-1$.

(ii) For k = 0 , after a simple calculation , we have

$A_{n-1}^{(0)} + A_{n-1}^{(2)} + \ldots + A_{n-1}^{(d-2)} = \dfrac{p^{n-1}(\kappa-1)}{2}$, $A_{n-1}^{(1)} + A_{n-1}^{(3)} + \ldots + A_{n-1}^{(d-1)} = -\dfrac{p^{n-1}(1+\kappa)}{2}$ where p = κ^2..

(iii) If u = d/2 is odd, $A_{n-1}^{(0)} + A_{n-1}^{(2)} + \ldots + A_{n-1}^{(d-2)} = -\dfrac{p^{n-1}(1+\tau)}{2}$,

$A_{n-1}^{(1)} + A_{n-1}^{(3)} + \ldots + A_{n-1}^{(d-1)} = \dfrac{p^{n-1}(\tau-1)}{2}$ where -p = τ^2.

Lemma 11. For $0 \le i \le n-1$, $0 \le k \le d-1$, then

(i) $B_i^{(k)} = 0$, if $0 \le i < n-1$.

(ii) $\sum B_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(\kappa+1)}{2}, & \text{if } k \text{ is even; } p = \kappa^2 \\ p^{n-1}\dfrac{(1-\kappa)}{2}, & \text{if } k \text{ is odd,} \end{cases}$ where d/2 is even.

(iii) $\sum B_{n-1}^{(k)} = \begin{cases} p^{n-1}\dfrac{(1-\tau)}{2}, & \text{if } k \text{ is even; } -p = \tau^2 \\ p^{n-1}\dfrac{(\tau+1)}{2}, & \text{if } k \text{ is odd,} \end{cases}$ where d/2 is odd.

Proof. As discussed in Lemma 11.

4. Dimension, generating polynomial and minimum distance of minimal cyclic codes of length $2p^n$

The dimension of minimal cyclic code Ω_s is the number of non-zeros of the generating idempotent θ_s; which is the cardinality of the cyclotomic coset C_s that is $\dim(\Omega_s) = |C_s|$. We denote the minimum distance of Ω_s by $d(\Omega_s)$.

Lemma 12. If C is the cyclic code of length m generated by g(x) and is of minimum distance d, then the code C is of length mk generated by $g(x)(1 + x^m + x^{2m} + \dots + x^{(k-1)m})$ is a repetition code of C repeated k times and minimum distance is kd.

Proof. Trivial.

4.1 Dimension, generating polynomial and minimum distance of Ω_0

By definition, $\dfrac{x^{2p^n}-1}{x-1} = 1 + x + x^2 + \dots + x^{2p^n-1}$ is the generating polynomial of Ω_0.Further, $\dim(\Omega_0) = |C_0| = 1$ and $d(\Omega_0) = 2p^n$.

4.2 Dimension, generating polynomial and minimum distance of Ω_{p^n}

By definition, the generating polynomial of Ω_{p^n} is $\dfrac{x^{2p^n}-1}{x+1} = -(1 - x + x^2 - \dots - x^{2p^n-1})$, thus $\dim(\Omega_{p^n}) = 1$ and $d(\Omega_{p^n}) = 2p^n$.

4.3 Dimension, generating polynomial and minimum distance of $\Omega_{2g^kp^j}$, for $0 \le j \le n-1$and $0 \le k \le d-1$.

We observe that, $\prod_{k=0}^{d-1} M^{(2g^kp^l)}(x) = (1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \dots + x^{(P-1)P^{n-j-1}})$.

Also, $x^{2p^n}-1=(x^{p^{n-j}}-1)(1+x^{p^{n-j}}+x^{2p^{n-j}}+\ldots+x^{(2p^j-1)p^{n-j}})$

$=$

$(x^{p^{n-j-1}}-1)(1+x^{p^{n-j-1}}+x^{2p^{n-j-1}}+\ldots+x^{(p-1)p^{n-j-1}})(1+x^{p^{n-j}}+x^{2p^{n-j}}+\ldots+x^{(2p^j-1)p^{n-j}})$.

Therefore, we have $\dfrac{x^{2p^n}-1}{\prod_{k=0}^{d-1} M^{(2g^k p^j)}(x)} = (x^{p^{n-j-1}}-1)(1+x^{p^{n-j}}+x^{2p^{n-j}}+\ldots+x^{(2p^j-1)p^{n-j}})$.

Let χ_j be the code of length $p^{n-j}q$ over GF(l) generated by $g(x)=(x^{p^{n-j-1}}-1)$. Then the minimum distance of χ_j is 2.

4.3.1. We shall further discuss some results for finding out the minimum distance of the minimal cyclic codes $\Omega_{2g^k p^j}$, for $0 \le j \le n-1$ and $0 \le k \le d-1$.

Lemma 13. Let C_1 and C_2 be cyclic code of length n over GF(l). Then C_1 and C_2 are equivalent under the mapping $\mu_g(i) \equiv ig (\text{mod } n)$ with gcd(n, g) = 1 and μ_g acting on R_n by $\mu_g(f(x)) \equiv f(x^g) (\text{mod } (x^n-1))$.

Theorem 4. For any integer t, $\theta_{st}(x) = \mu_{s^{-1}}(\theta_t(x))$ if gcd(s, m) =1, where $\theta_s(x)$ is the generating idempotent of irreducible cyclic code Ω_s.

Proof. See [1, Theorem 3].

Theorem 5. For each j, $0 \le j \le n-1$ and $0 \le k \le d-1$

(i) $\Omega_{2g^k p^j}$ are equivalent codes.

(ii) The minimum distance of each $\Omega_{2g^k p^j}$ is at least $4p^j$.

Proof. (i) In view of Theorem 4 and Lemma 13, the proof follows trivially.

(ii) Let χ_j^* be the cyclic code of length $2p^n$, generated by $\dfrac{x^{2p^n}-1}{\prod_{k=0}^{d-1} M^{(2g^k p^j)}(x)}$.

Then χ_j^* is a repetition code of χ_j repeated $2p^j$ times and its minimum distance is $4p^j$. Further, $\chi_j^* = \oplus_{k=0}^{d-1}\Omega_{2g^k p^j}$, thus $\Omega_{2g^k p^j}$ is sub code of χ_j^*. Therefore, the minimum distance of $\Omega_{2g^k p^j}$ is at least $4p^j$.

Theorem 6. For each j, $0 \le j \le n-1$ and $0 \le k \le d-1$

(i) $\Omega_{g^k p^j}$ are equivalent codes.

(ii) The minimum distance of each $\Omega_{g^k p^j}$ is at least $4p^j$.

Proof. The proof follows on the similar lines as Theorem 5.

5. Example. Let p = 11, n = 1, *l* = 3. Then length of the cyclic code is 22, g = 7 and d = 2.
The 3-cyclotomic cosets modulo 22 are given by:
$C_0 = \{0\}$, $C_{11} = \{11\}$, $C_1 = \{1, 3, 5, 9, 15\}$, $C_2 = \{2, 6, 8, 10, 18\}$
$C_7 = \{7, 13, 17, 19, 21\}$, $C_{14} = \{4, 12, 14, 16, 20\}$.
Explicit expression for the primitive idempotents of the irreducible cyclic code of length 22 are given by:
$\theta_0(x) = 1 + x + x^2 + \ldots + x^{21}$ $\quad$ $\theta_1(x) = 2 + \sigma_1(x) + \sigma_{11}(x) - \sigma_{14}(x)$
$\theta_2(x) = 2 - \sigma_7(x) - \sigma_{11}(x) - \sigma_{14}(x)$ $\quad$ $\theta_7(x) = 2 - \sigma_2(x) + \sigma_7(x) + \sigma_{11}(x)$
$\theta_{11}(x) = 1 - \sigma_1(x) + \sigma_2(x) - \sigma_7(x) - \sigma_{11}(x) + \sigma_{14}(x)$ $\quad$ $\theta_{14}(x) = 2 - \sigma_1(x) - \sigma_2(x) - \sigma_{11}(x)$
The minimal ternary cyclic codes of length 22 have the following parameters:

Code	Dimension	Minimum Distance	Generating Polynomial
Ω_0	1	22	$1 + x + x^2 + \ldots + x^{21}$
Ω_{11}	1	22	$1 - x + x^2 - \ldots + x^{21}$
χ_j^*	10	4	$(x-1)(1+x^{11})$
χ_j^{**}	10	4	$(x-1)(1-x^{11})$

Note that Ω_2, Ω_{14} and Ω_1, Ω_7 are sub codes of χ_j^* and χ_j^{**} respectively. Therefore, the minimum distance of Ω_2, Ω_{14} and Ω_1, Ω_7 is at least 4.

References

[1] A.Sahni and P.T.Sehgal,"Minimal Cyclic Codes of length $p^n q$," Finite Fields Appl. 18 (2012) 1017-1036.

[2] F.J. Mac Williams & N.J.A. Sloane; The Theory of Error Correcting Codes Bell Laboratories Murray Hill NJ 07974 U.S.A.

[3] G. K. Bakshi and Madhu Raka, "Minimal Cyclic Codes of Length $p^n q$," Finite Fields Appl. 9(4) (2003) 432-448.

[4] M. Pruthi and S.K. Arora, "Minimal Cyclic Codes of Prime Power Length," Finite Field and their Application, 3, 99-113(1997).

[5] M.Raka;G.K. Bakshi ; A. Sharma,V.C. Dumir,. “Cyclotomic numbers and primitive idempotents in the ring $\frac{GF(q)[x]}{(x^{p^n}-1)}$,” Finite Field & Their Appl.3 no.2(2004) 653-673.

[6] R. Singh and M. Pruthi, “ Primitive idempotents of quadratic residue codes of length $p^n q^m$,” Int.J.Algebra 5(2011) 285-294.

[7] S. Batra and S.K. Arora, “Minimal quadratic residue cyclic codes of length p^n (p odd prime),” Korean J. Comput & Appl. Math. Vol. 8(3) (2001), 531-547.

[8] S.Batra and S.K. Arora, “Some cyclic codes of length $2p^n$ (p odd prime),” Design Codes Cryptography , Vol. 57(3) (2010).

[9] S.K. Arora and M. Pruthi, “Minimal Cyclic Codes Length $2p^n$,” Finite Field and their Applications, 5, 177-187(1999).

[10] Vera Pless, “Introduction to the Theory of Error-Correcting Codes”, Wiley-Intersci. Ser. Discrete Math. Optim., (1998).

Received: November, 2012